PENERAPAN METODE ELGAMAL, DATA ENCRYPTION STANDARD DAN RSA UNTUK PENCEGAHAN DUPLIKASI KARTU KREDIT DAN KARTU DEBIT

[1]Dhian Sweetania, ST., MMSI. [2]Yuli Maharetta Arianti, SKom., MMSI.
[1,2]Jurusan Sistem Informasi
Universitas Gunadarma
Jl. Margonda Raya 100 Pondok Cina, Depok 16424
[1,2] {dhian_sweetania, yuli_maharetta}@staff.gunadarma.ac.id

ABSTRAK

Perkembangan teknologi dalam dunia perbankan membuat kemudahan-kemudahan yang diberikan kepada klien sebagai bentuk pelayanan yang maksimal agar membantu para klien dalam melakukan transaksi tanpa perlu membawa uang kas. Bank mengeluarkan kebijakan pemakaian kartu kredit dan kartu debit sebagai pengganti uang kas untuk memudahkan klien agar tidak perlu repot dan terancam bahaya karena membawa uang dalam jumlah yang besar. Kartu debit dan kredit di Indonesia masih menggunakan magnetic strip yang rentan mendapat ancaman pemalsuan data dan duplikasi kartu. Untuk itu di kembangkan kartu yang menggunakan chip yang sulit di tembus oleh para penjahat. Chip yang digunakan ini didalamnya menerapkan pembangkit kunci dengan bilangan acak metode algoritma ELGAMAL, DES, dan RSA. Hasil output algoritma ini pun tetap disimpan dalam chip kartu privat tersebut.

Kata kunci :*Kartu Kredit dan Debit,duplikasi,magnetic strip,chip, algoritma ELGAMAL, DES, RSA*

1. PENDAHULUAN

PT Bank Danamon Indonesia, (Tbk) membidik sebanyak 3 juta pengguna kartu kredit dan debit pada 2014 atau tumbuh 20 persen dibandingkan 2013 sebanyak 2,5 juta pengguna kartu. Direktur Consumer Banking Danamon Michellin Triwardhany dilansir Antara di Jakarta, Senin (2/12).menuturkan, untuk memenuhi target penggunaan tersebut, pihaknya akan melakukan beberapa strategi yakni dengan melakukan edukasi pada masyarakat terkait pentingnya penggunaan kartu debit atau kredit ketimbang membawa uang tunai. Berdasarkan data, jumlah pengguna kartu kredit dan debit pada bank tersebut saat ini sebanyak 2,5 juta, di mana jumlah pengguna kartu debit sebanyak 700.000 dan pengguna kartu debit sebanyak 2 juta pengguna [9]

Kartu kredit dua sisi mata uang, selain dibutuhkan namun juga rawan untuk disalah gunakan. Hal ini yang ditangkap oleh Bank Indonesia, bahwa kejahatan kartu kredit atau fraud masih mendominasi untuk kategori Alat Pembayaran Menggunakan Kartu (APMK). Menurut Deputi BI, Ronald Waas hingga Mei 2012, kejahatan perbankan elektronik telah mencapai 1.009 kasus dan kebanyakan adalah terhadap kartu plastik. Kerugiannya pun relative cukup besar, yaitu Rp. 2,37 miliar. Masih menurut Ronald Waas, diantara sekian banyak kejahatan kartu kredit**,** counterfeit (pencurian identitas dan CNP (Card Not Present, fraud dimana kartu kredit tidak berada di tangan pelaku) adalah yang paling sering dilakukan. Tercatat terjadi 402 kasus counterfeit dengan kerugian Rp. 1,14 miliar dan 458 kasus CNP dengan kerugian Rp. 545 juta. Yang membuat miris, kejahatan ini dialami oleh hampir dari semua penerbit kartu kredit. Meskipun kejahatan kartu kredit masih marak, namun untuk peringkat fraud global, Indonesia ternyata tidak terlalu mengkhawatirkan. Diantara negara-negara di Asia Pasifik, peringkat Indonesia masih berada di bawah. Menurut Mastercard, peringkat Indonesia masih berada di level kedua terbawah. Sedangkan menurut VISA, peringkat kita masih berada di posisi ketiga

terbawah. Peringkat ini jauh lebih baik jika dibandingkan negara tetangga, seperti Singapura dan Malaysia. Meskipun peringkat fraud Indonesia masih relatif rendah, namun jika terus dibiarkan, bisa jadi kejahatan kartu kredit akan semakin meraja lela. Salah satu usaha BI untuk mencegahnya adalah dengan menerapkan 6 digit PIN pada kartu kredit yang selambatnya dilakukan pada akhir 2014. [10]

2. LANDASAN TEORI

Pengertian Kartu Kredit

Kartu Kredit adalah salah satu alat pembayaran paling mutakhir setelah cek dan giro yang bersifat tidak tunai.Kartu krdit dibuat dari plastik dengan ukuran standar tertentu dan berisikan data nomor kartu yang terekam dengan magnetic stripe pada bagian belakang kartu. Pada bagian depan kartu terdapat nama dan nomor pemegang kartu yang dicetak timbul,juga terdapat tanggal masa berlaku kartu tersebut.

Pengertian Kartu Debit

Kartu debit adalah sebuah kartu pembayaran secara elektronik yang diterbitkan oleh Bank. Kartu ini dapat berfungsi sebagai pengganti pembayaran dengan uang tunai.Kartu ini mengacu pada saldo tabungan bank anda di bank penerbit tersebut. Fungsi dari kartu debit adalah untuk memudahkan pembayaran ketika berbelanja tanpa harus membawa uang tunai. Dalam beberapa kasus, nomor rekening primer diberikan secara eksklusif untuk digunakan di Internet dan tidak ada kartu fisik.

Pengertian Chip

Berdasarkan media yang digunakan untuk merekam ‘nilai uang’ yang telah dikonversi ke dalam format elektronis,

Produk e-money umumnya dikategorikan atas dua kelompok yaitu:

1. Card-based product (prepaid card)
   - E-money dalam bentuk card-based product sering juga disebut sebagai electronic purses. Card-based product pada prinsipnya dimaksudkan untuk pembayaran yang bersifat langsung (face to face), namun demikian saat ini beberapa card-based product juga dapat digunakan untuk pembayaran via internet dengan menambahkan alat tertentu pada komputer pengguna.Jenis produk ini menggunakan media kartu dengan teknologi integrated circuit (IC) atau dikenal dengan ‘IC card’ yang mengandung microprocessor chip (chip). IC cards dapat digolongkan menjadi dua jenis yaitu :smart cards dan memory cards. Smart card telah memiliki fungsi untuk melakukan proses data serta fungsi penyimpanan.
   - Sementara memory card hanya memiliki fungsi untuk penyimpanan data. Saat ini, produk e-money yang berbasis kartu pada umumnya menggunakan teknologi smart card, mengingat fungsi ’dataprocessing’ sangat dibutuhkan untuk melakukan proses perhitungan.

Smart card sendiri dapat digolongkan lagi menjadi 2 (dua) type yaitu :

- contact type, dimana dalam penggunaannya kartu harus diinsert ke dalam mesin pembaca (card-reader); dan
- contactless type, dimana dalam penggunaannya kartu tidak harus di-insert ke dalam card-reader, melainkan cukup diarahkan/didekatkan ke alat pembaca (tanpa harus menyentuh).

Secara fisik, smart card merupakan kartu plastik dimana sebuah IC chip ditanamkan ke dalam kartu tersebut. Di dalam chip tersebut terdapat operating system dan aplikasi (sotfware) yang di-install pada saat proses produksi (manufacturing) chip dimaksud. Microprocessor chip inilah yang berfungsi sebagai pusat pengendalian seluruh transaksi yang mempunyai kemampuan untuk melakukan perhitungan-perhitungan serta perekaman data.Spesifikasi fisik dan elektronik dari suatu produk smart card umumnya mengacu pada standard internasion

al (ISO/EMV).

2. Software-based product (prepaid software)

- Sering disebut juga digital cash. Produk e-money yang masuk dalam kelompok ini pada prinsipnya merupakan suatu aplikasi (software) yang kemudian di-install ke dalam suatu Personal Computer (PC) yang dijalankan dengan operating system yang standard.Produk ini dikembangkan untuk melakukan transaksi melalui suatu jaringan komputer (internet). Meskipun demikian, beberapa card-based product (seperti Mondex) juga sudah dapat digunakan untuk melakukan transaksi melalui internet dengan menggunakan alat bantu tertentu [11]

Features ini mencakup proteksi yang bersifat logical (software protection) maupun fisikal (hardware protection).

1) Software protection, merupakan proteksi dalam bentuk aplikasi (software) dan cryptography.
2) Hardware protection, merupakan proteksi secara fisik yang dibuat pada saat proses produksi chip/komputer yang bertujuan untuk mencegah pihak luar mengetahui dan melakukan perubahan terhadap komponen-komponen chip.

Bentuk proteksi ini antara lain dapat berupa :

1) Ukuran chip's wiring yang digunakan. Semakin kecil ukuran wiring akan semakin sulit untuk menganalisa komponen suatu chip.
2) External coating serta internal wiring yang berlapislapis (multiple layers) sedemikian rupa sehingga sulit untuk dilepas satu per satu tanpa merusak chip itu sendiri.
3) Pemasangan sensor di dalam chip untuk mendeteksi adanya panas, sinar dan arus listrik yang tidak normal serta untuk membuat chip tidak beroperasi secara otomatis apabila ada upaya kejahatan yang sekaligus memberikan bukti adanya upaya kejahatan tersebut (tamper-evident).
4) Layout komponen chip serta data yang bersifat sensitive dibuat secara scattered (menyebar), sehingga sulit untuk dianalisa.

Pengertian Magnetic stripe

Strip magnetik adalah pita/strip gelap di bagian belakang kartu bank. Strip ini terbuat dari partikel magnetik tipis yang ditanam di dalam damar.

a. Proses operasi

Selama proses enkode, partikel ini diisi dengan magnet dengan arah kutub Utara atau Selatan. Setiap karakter pada strip di-enkode dengan himpunan angka-angka 1 dan 0. Polaritas partikel magnetik diubah untuk menunjukkan masing-masing bit tersebut.Mengubah magnetisasi setiap partikel pada strip akan membantu meng-enkode informasi biner yang akan diuraikan sandinya oleh pembaca yang sesuai.

b. Koersivitas

Koersivitas merujuk pada kekuatan medan magnet yang diperlukan untuk mengedit data yang dimasukkan ke dalam strip magnetik. Ada dua jenis trip magnetik dengan tingkat koersitivitas yang berbeda: Strip magnetik HiCo (Koersitivitas Tinggi) memberikan tingkat keamanan yang lebih tinggi terhadap potensi kerusakan dari medan magnet pihak ketiga. Strip LoCo (Koersitivitas Rendah) adalah medan magnet yang lebih peka terhadap medan magnet pihak ketiga, tetapi lebih murah.

Langkah Pengamanan (*security measures)*

Langkah pengamanan dapat dikelompokkan sebagai berikut:

- Preventive measures, bertujuan untuk memastikan bahwa ancaman kejahatan terhadap komponen-komponen dalam sistem dapat dihalangi/dicegah semaksimal mungkin sebelum terjadi.
- Detection measures, bertujuan untuk memberikan peringatan (alert) kepada issuer atau operator akan terjadinya

fraud serta untuk mengidentifikasi lokasi terjadinya fraud tersebut.
- Containment measures, bertujuan untuk membatasi/mengurangidampak kerugian akibat dari suatu kejahatan yang sudah terjadi.

Bentuk-bentuk security measures yang dapat diterapkan untuk mencegah terjadinya kejahatan dalam e-money antara lain:

a. Menggunakan chip yang tamper-resistance
   - Pada sistem e-money yang berbasis kartu, instrument yang digunakan oleh konsumen berupa *smart card* yang mengandung chip. Sementara instrument yang digunakan oleh merchant dapat berupa smartcard atau secure application modul (SAM) yang terintegrasi pada terminal merchant. Keamanan pada kedua instrument ini sangat ditentukan oleh chip/computer yang terdapat di dalam smart card maupun terminal merchant.
   - Tamper resistance features bertujuan untuk melindungi data dan aplikasi yang tersimpan dalam chip/komputer dari upaya pihak pihak tertentu yang ingin melakukan perubahan terhadap data dan aplikasi tersebut atau mempelajari aplikasi yang digunakan untuk maksud-maksud tertentu.

b. Cryptography
   - Merupakan suatu aplikasi yang bersifat matematis yang bertujuan untuk memberikan security level tertentu. Teknik ini memberikan proteksi yang bersifat logical untuk menjamin confidentiality, authenticity, dan integritydari instrumen, data dan komunikasi yang digunakan dalam melakukan transaksi.

Ada beberapa teknik cryptographic yang dapat digunakan untuk tujuan yang berbeda :

- Enkripsi, mampu menjamin confidentiality data selama proses transmisi atau proses penyimpanan.
- Digital Signatures, merupakan teknik yang dapat digunakan untuk menjamin authenticity instrument (kartu atau terminal) yang digunakan dalam bertransaksi. Selain itu,digital signatures juga bisa digunakan untuk mencegah repudiation (penyangkalan) dari salah satu pihak yang bertransaksi.
- Message Authentication Codes, merupakan teknik untuk menjamin integritas data/message yang dipertukarkanantar dua instrument (misalnya dari kartu ke terminalmerchant) dengan mendeteksi apakah telah terjadiperubahan data/message sebelum sampai ke tempat tujuan.

Teknik cryptography sangat bergantung pada algoritma matematika yang digunakan serta parameter yang dikenalsebagai kunci (key). Saat ini tersedia beberapa jenis algoritma cryptography.

Secara umum, algoritma dibedakan antara kunci simetris dan kunci asimetris (kunci publik/public key). Algoritma simetris menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi. Sementara algoritma asimetris memerlukan pasangan public key dan private key dalam melakukan enkripsidan dekripsi data. Data yang di-enkrip dengan public key hanyadapat di-dekrip dengan private key pasangannya. Sebaliknya data yang di-enkrip dengan private key hanya dapat dibukadengan public key pasangannya. Public key dapat diketahui oleh orang lain, sedangkan private key hanya disimpan pada instrument milik individu, sehingga lebih sulit untuk diserang olehorang lain. Proses yang menggunakan kunci asimetrismemerlukan waktu yang lebih lama dari pada yangmenggunakan kunci simetris.Sistem yang menggunakan cryptography dapat diserang dengan memanfaatkan kelemahan algoritma yang digunakan, mencuri kunci rahasia atau

dengan cara coba-coba (brute force attack).

Berkaitan dengan algoritma, semakin panjang kunci yangdigunakan maka akan semakin sulit dan mahal cost yang harus dikeluarkan untuk memecah algoritma dengan cara coba-coba. Namun demikian, semakin panjang kunci yang digunakan akan semakin lama waktu proses yang diperlukan yang tentunya mempengaruhi tingkat kualitas smart card yang digunakan.
Algoritma yang umumnya digunakan untuk penyelenggaraan e-money saat ini adalah DES (Data EncryptionStandard) dan triple-DES serta RSA (Rivest-Shamir-Adlemen).Panjang algoritma asymetris yang digunakan berkisar antara 512bits s/d 2.048 bits.

Untuk sistem yang menggunakan cryptographic asimetris, diperlukan adanya Certification Authorities (CA). Keberadaan CA ini pada prinsipnya merupakan sentralisasi database yang melakukan sertifikasi, menyimpan serta mendistribusikan publickey dan informasi identitas pemilik private key yang merupakanpasangan dari public key tersebut. [16]

3. METODE PENELITIAN

Dalam penelitian ini meneliti tentang usaha pencegahan duplikasi yang terjadi pada kartu kredit dan kartu debit dengan cara pencurian data melalui skimmer.Data pada penelitian ini didapat dari catatan-catatan dan laporan-laporan mengenai tindakan kejahatan yang telah terjadi.

PEMBAHASAN

Cara Para Penjahat Mencuri Data
Pada kejadian umum para pelaku kejahatan akan mengincar targetnya dan mencari tahu informasi mengenai nomor pin atau nomor kartu kredit korban untuk selanjutnya menduplikasi data-data yang didapat dan dimasukkan pada kartu palsu yang dibuat semirip mungkin dengan yang asli.
Ada beberapa cara yang dilakukan untuk mendapatkan data nomor pin korban yaitu dengan cara :

1. Pelaku mengintip calon korban dari belakang antrian lewat bahu korban yang sedang melakukan transaksi pada mesin ATM, ini bisa terjadi pada tempat-tempat seperti di Mall atau di lobby bank yang letak ATM-nya terbuka. Dan si pelaku pasti orang yang punya daya ingat tinggi karena dapat merekam nomor PIN dikepala hanya dengan sekilas.
2. Si pelaku kejahatan memasang kamera kecil (Spycamera) dan Card reader pada mesin ATM. Mesin card reader berfungsi untuk merekam data dari magnetic stripe kartu ATM, sementara kamera kecil yang tersembunyi digunakan untuk mengintip atau merekam nomor PIN korban saat menggunakan keypad ATM.

Adapun juga cara untuk mendapatkan data pada kartu kredit dan kartu debit(ATM) yaitu

1. Dengan membaca record terakhir pada mesin ATM, cara ini lebih sulit dilakukan dibandingkan dengan cara yang lainnya dan lebih berbahaya. Caranya yaitu pelaku membuat kartu elektrik yang dibuat dan diformat untuk dapat membaca transaksi terakhir pada mesin ATM.
2. Data dan nomor awalnya didapat dengan cara Skimming artinya merekam secara elektronik data pada magnetic stripe skimming ini biasanya di kerjakan dengan suatu alat sebesar bungkus rokok dan tergantung ada berbagai model yang dijual di pasaran, biasanya si pelaku kejahatan dalam mencuri data dan nomor dari kartu kredit asli akan menitipkan Skimming tersebutdiRestoran, hotel, Toko, atau tempat-tempat pembayaran dengan istilah gesek, yang artinya harus ada keterlibatan orang dalam dari tempat-tempat tersebut, biasanyasi kasir menyembunyikan SKIMMER di bawah meja dan melakukan dua kali penggesekan tanpa sepengetahuan pemilik kartu.

3. Cara lain pencurian data pemilik kartu kredit asli adalah bisa dengan cara memasangsemacam CHIP pada terminal POS (point of sale) yaitu sebuah alat gesek kartu kredit yang digunakan unbtuk pembayaran, pada restoran, toko, hotel, super market, dan si pelaku kejahatan disini bisa petugas service terminal POS, karyawan pada terminalPOS, atau orang lain yang menitipkan. Intinya bahwa CHIP harus dipasang oleh petugas yang menangani terminal POS, misalkan pada saat service.

Pengembangan Chip Pada Kartu Sebagai Antisipasi Dari Penduplikasian Data Kartu Kredit dan Debit

Cara pelaku kejahatan pencuri data kartu kredit dan debit sebagian besar bekerja pada pemakai kartu yang masih menggunakan magnetic stripe. Hal itu terjadi karena magnetic stripe masih memiliki tingkat keamanan yang rendah dan sudah banyak alat yang dapat mendeteksi data yang tersimpan pada pita tersebut.Atas dasar itu maka telah dikembangkan chip yang dapat dipasangkan pada kartu dan sudah mulai diterapkan pada kartu kredit dan kartu debit. Chip ini memiliki tingkat keamanan berlapis dan alat-alat penduplikasi data yang digunakan pada magnetic stripe tidak berfungsi pada chip.

Perbedaan antara magnetic stripe dengan chip yaitu data dari magnetic stripe bisa dikopi, tetapi dari chip tidak bisa. Selain itu, kartu berbasis chip memiliki kapasitas penyimpanan data yang lebih besar. Bank dapat menambahkan fasilitas khusus pada kartu, sehingga pemilik kartu mendapatkan banyak keunggulan.Misalnya, fungsi kartu kredit sekaligus media akses dan pembayaran otomatis terminal IP-Phone.

4. PENJELASAN CARA KERJA PADA CHIP DAN ALGORITMA

Algoritma yang digunakan dalam pengamanan informasi yang tersimpan di dalam smart card meliputi :

Algoritma ElGamal

Algoitma ElGamal merupakan algoritma dalam kriptografi yang termasuk algoritma asimetris. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini termasuk ke dalam algoritma block chiper, yaitu melakukan proses enkripsi pada blok-blok plainteks yang akan menghasilkan blok-blok chiperteks yang kemudian digabungkan menjadi hasil secara keseluruhan. Algoritma pembangkitan kunci dalam algoritma El-Gamal dapat dijelaskan sebagai berikut :

1. Pilih sembarang bilangan prima p (p dapat di-share di antara anggota kelompok)

2. Pilih dua buah bilangan acak, g dan x, dengan syarat g < p , yang dalam hal ini 1 √ k √ p – 2.
3. Hitung y = gx mod p.

Hasil dari algoritma ini: Kunci public : tripel (y, g, p) Kunci privat : pasangan (x, p) Algoritma enkripsi yang digunakan dalam algoritma El-Gamal dapat dijelaskan sebagi berikut :

1. Susun plainteks menjadi blok-blok m1, m2,..(nilai setiap blok di dalam selang [0, p – 1]).

2. Pilih bilangan acak k, yang dalam hal ini 1 √ k √ p – 2. 3. Setiap blok m dienkripsi dengan rumus a = gk mod p b = ykm mod p Pasangan a dan b adalah cipherteks untuk blok pesan m. Jadi, ukuran cipherteks dua kali ukuran plainteksnya.

Algoritma dekripsi yang digunakan dalam algoritma El-Gamal dapat dijelaskan sebagi berikut :

1. Gunakan kunci privat x untuk menghitung (ax)– 1 = ap – 1 – x mod p

2. Hitung plainteks m dengan persamaan: m = b/ax mod p = b(ax)– 1 mod p

Algoritma RSA

Algoitma RSA merupakan algoritma dalam kriptografi yang termasuk algoritma kunci-publik yang paling terkenal dan paling banyak diaplikasikan dalam berbagai

teknologi yang digunakan saat ini. Algoritma RSA terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma pembangkitan kunci dalam algoritma RSA dapat dijelaskan sebagai berikut : 1. Pilih dua bilangan prima p ≠ q secara acak dan terpisah untuk tiap-tiap p dan q. 2. Hitung N dengan persamaan: N = p q. 3. Hitung φ dengan persamaan: φ = (p-1)(q-1). 4. Pilih bilangan bulat (integer) antara satu dan φ (1 < e < φ) yang juga merupakan coprime dari φ. 5. Hitung d dengan persamaan : de≡ 1 (mod φ). Hasil dari algoritma ini: Kunci public : pasangan (N,e) Kunci privat: pasangan (N,d)

Algoritma enkripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut :

1. Susun plainteks menjadi blok-blok m1, m2, , (nilai setiap blok di dalam selang [0, p – 1].

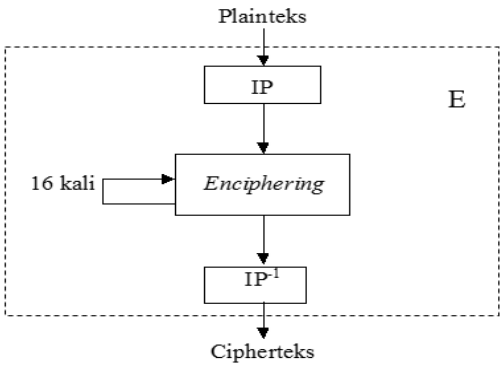
2. Hitung chipertext ci dengan rumus : ci = mi e mod N Algoritma dekripsi yang digunakan dalam algoritma RSA dapat dijelaskan sebagai berikut :

   a. Gunakan kunci privat untuk menghitung mi = ci d mod N

   b. Carilah nilai m dengan rumus cd ≡ (mie) d ≡ mied mod N Nilai m merupakan pesan semula yang dikirimkan.

Algoritma DES

Algoritma DES merupakan algoritma dalam kriptografi yang termasuk algoritma kunci-simetri dan tergolong ke dalam jenis block chiper. Dalam algoritma DES, setiap blok akan diporses ke dalam 16 putaran di mana setiap putaran akan menggunakan kunci internal yang berbeda. Kunci internal itu sendiri dibangkitkan dengan menggunakan kunci eksternal. Setiap blok akan mengalami permutasi awal (IP), 16 putaran enchipering, dan inversi pemutaran awal (IP-1) yang dapat digambarkan melalui skema berikut :

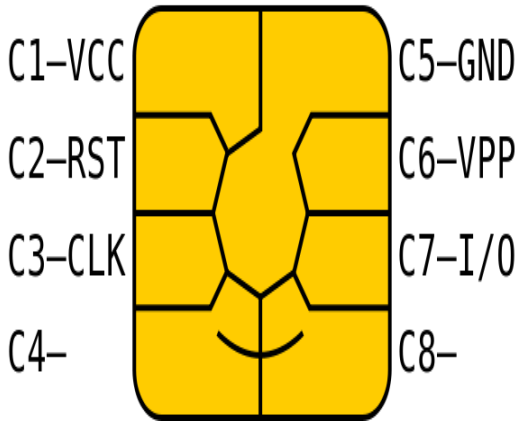


Gambar 1. TABEL DES

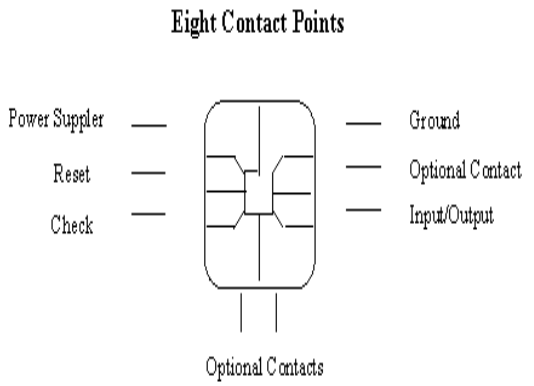
Pembangkitan kunci internal dalam algoritma DES dibangkitkan dari kunci eksternal (64 bit) yang diberikan oleh pengguna. Kunci eksternal itu kemudian masuk ke proses pembangkitan kunci internal sebanyak 16 kali. Kunci internal yang dimaksud adalah kunci yang dihasilkan dari setiap putaran.

Penjelasan CHIP pada Kartu Kredit dan Debit

Pada umumnya ukuran smartcard yang digunakan adalah 8 KB dan 16 KB.Untuk sistem yang menggunakan pasangan kunci privat dan publik membutuhkan smartcard dengan memori minimal 16 KB karena untuk menyimpan kunci privat dan tanda tangan digital membutuhkan memori sebesar 2 KB dan komputasi enkripsi / dekripsi yang dilakukan membutuhkan memori yang cukup besar. Data medical record yang disimpan disesuaikan dengan kapasitas memori smartcard.



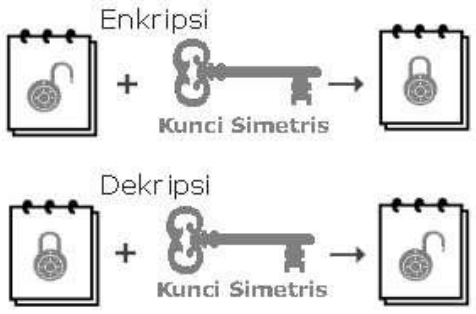
Gambar 2. Bagian-Bagian pada CHIP 1



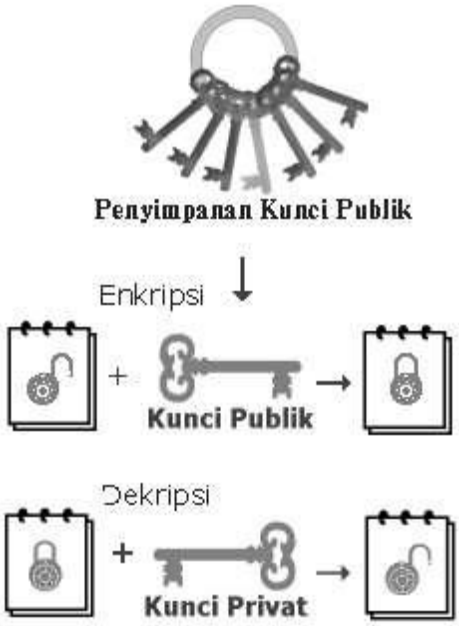
Gambar 3. Bagian-Bagian CHIP 2

Perangkat lunak aplikasi yang digunakan untuk membaca dan menulis data pengguna dalam smartcard haruslah berasal dari pihak yang sama dengan pembuat smartcard, jadi smartcard dari suatu vendor tertentu tidak dapat dibaca dengan menggunakan perangkat lunak aplikasidari vendor lain . Pihak yang menerbitkan kartu dan layanan aplikasi disebut card centre.Card centre bertanggung jawab ada semua kartu yang diterbitkannya.

Sistem keamanan dalam smartcard menggunakan mekanisme enkripsi kunci asimetris atau kunci simetris. Untuk mekanisme enkripsi kunci asimetris menggunakan pasangan kunci privat dan publik, kunci publik boleh diketahui oleh pihak lain sedangkan kunci privat dan algoritma yang digunakan untuk membuat kedua kunci tersebut dirahasiakan. Sedangkan untuk mekanisme kunci simetris, kunci simetris tersebut disimpan dalam perangkat lunak pembuat layanan kartu.



Gambar 5. Kunci Simetris



Gambar 6. Kunci Asimetris

Semua informasi pengguna yang bukan disimpan dalam smartcard melainkan yang disimpan di basis data dan dapat diakses oleh dokter secara on-line. Keamanan waktu pengiriman dan penyimpanan informasi dilakukan dengan mengenkripsi setiap data yang dikirim lewat jaringan dengan kunci sesi yang telah disepakati oleh kedua belah pihak. Pengiriman kunci sesi dilakukan dengan mengenkripsi kunci sesi tersebut dengan kunci publik penerima kunci.Hal ini menjamin bahwa hanya penerima kunci yang berwenang yang dapat membuka kunci sesi tersebut, karena hanya pemilik kunci publik saja yang dapat mendekripsi data dengan kunci privat miliknya. Setiap data yang disimpan dalam basis data di card centre atau pada basis datanya juga dienkripsi dengan menggunakan kunci simetris atau asimetris milik card centre atau sehingga pengakses data pengguna yang tidak diinginkan, tidak dapat mengerti isi data pengguna walaupun dia berhasil mendapatkan data pengguna yang terenkripsi.

Kunci-kunci yang dibutuhkan oleh smartcard untuk menjaga keamanan data:

1. PIN : untuk memeriksa apakah pemakai memang pemegang sah dari smartcard (otentikasi).

2. Identitas pemberi layanan atau kode perusahaan : untuk memastikan agar hanya smartcard yang mempunyai kode dari perusahaan tersebut yang bisa menggunakan layanan. Jadi smartcard yang dikeluarkan oleh perusahaan pemberi layanan A tidak dapat digunakan untuk mengakses layanan dari perusahaan B, kecuali jika kedua kode dari perusahaan tersebut di tulis di dalam smartcard. Kode perusahaan sama untuk semua smartcard dari perusahaan tersebut. Kode perusahaan hanya diketahui oleh perusahaan tersebut dan sulit untuk diketahui oleh pihak lain.

3. Kunci simetris : untuk mengenkripsi data dalam smartcard supaya tidak bisa dibaca oleh pihak yang tidak berwenang. Kunci simetris ini tidak diketahui oleh pemakai maupun pihak luar, hanya diketahui oleh penerbit kartu atau perangkat lunak aplikasi. Sehingga jika seorang penyerang berhasil memperoleh nilai PIN dan kode perusahaan maka penyerang tersebut tidak dapat melakukan dekripsi data yang ada di dalam smartcard.

4. Pasangan kunci privat dan kunci publik: untuk membuktikan identitas yang handal pada waktu pemilik smartcard menggunakan layanan berupa pengiriman data melalui jaringan komputer. Pasangan kunci privat dan kunci publik ini disimpan di dalam smartcard secara terenkripsi dengan menggunakan kunci simetris. Akses baca kunci tersebut dijaga oleh kode perusahaan. Dengan demikian walaupun nilai PIN dan kode perusahaan diketahui, nilai kunci privat dan kunci publik tidak diketahui oleh si penyerang karena si penyerang tidak dapat mengetahui kunci simetris untuk melakukan dekripsi terhadap kunci-kunci tersebut. Kunci publik diketahui oleh umum tetapi disimpan juga di dalam kartu karena kedua kunci tersebut digunakan untuk melakukan verifikasi bahwa kedua kunci tersebut merupakan pasangan kunci yang sebenarnya.

Proses verifikasi tersebut adalah :

- Dekripsi kunci privat dan kunci publik dengan menggunakan kunci simetris sehingga diperoleh nilai kunci privat dan kunci publik.

- Enkripsi sebuah pesan dengan menggunakan kunci publik.

- Dekripsi pesan yang terenkripsi tersebut dengan kunci privat.

- Bandingkan pesan awal dengan pesan yang diperoleh. Jika sama maka kedua kunci tersebut memang pasangan yang sebenarnya.

Untuk membuktikan kunci publik yang sah maka digunakan sertifikat digital yang berisi kunci publik tersebut.Supaya penyerang tidak dapat memasukkan program untuk mencuri data dan menambah alat-alat untuk melakukan physical external attack atau membuat sebuah dumb mouse maka antara terminal komputer dan smartcard reader harus didedikasikan untuk aplikasi smartcard tersebut, seperti yang terjadi untuk mesin pengambilan uang “ATM”.
Berikut ini merupakan perintah untuk mengisi sebuah smart card :

1. Periksa apakah ada card reader yang terhubung ke komputer.
2. Beri perintah card reader untuk menyalakan power dari smartcard.
3. Ambil data dari pemakai dan buat menjadi kode PIN.
4. Hasilkan kunci publik, kunci privat dan hash dari kunci privat, kunci publik dan serial number. Karena menggunakan public key card maka membangkitkan bilangan acak untuk kunci dan pelaksanaan algoritma RSA, algoritma DES maupun algoritma ELGAMAL dapat dilakukan di dalam smartcard. Sehingga kunci privat yang dihasilkan

tidak pernah keluar dari smartcard karena begitu kunci tersebut dihasilkan di dalam smartcard langsung disimpan di dalam smartcard.

5. Enkripsi kunci publik, kunci privat dan nilai hash dengan menggunakan kunci simetris yang dimiliki oleh perangkat lunak. Komputasi ini dilakukan di dalam smartcard.
6. Buat file untuk menyimpan kunci privat dan publik yang dihasilkan.
7. Simpan kunci ke file di smartcard.
8. Beri perintah kepada reader untuk mematikan power dari smartcard.

5. PENUTUP

Dari beberapa kasus yang terjadi pada penduplikasian data kartu kredit dan debit banyak faktor-faktor kelemahan dari sistem keamanan yang melindungi masih lemah. Kelemahan keamanan karena pada magnetic stripe data dapat dicuri dengan mudah dan para pelaku bisa membuat kartu palsu dengan memasang alat cetak magnetic stripe.Keamanan pun akhirnya ditingkatkan dengan mengembangkan teknologi baru yaitu chip. Chip ini dipasangkan pada kartu sehingga data lebih aman karena chip memakai sistem keamanan berlapis. Keamanan pada teknologi perlindungan data pada kartu sebenarnya sudah baik tetapi para pelaku kejahatan selalu mengembangkan tehnik-tehnik baru untuk membobol sistem keamanan karena itu keamanan harus selalu berkembang demi bisa melindungi data para nasabah.

6. DAFTAR PUSTAKA

1. D. Boneh, R. DeMillo and R. Lipton, On the Importance of Checking Cryptographic Protocols for Faults, Journal of Cryptology, Springer-Verlag, nol. 14, no. 2, pp. 101–119, 2001
2. N. Manaresi, A. Romani, G. Medoro, L. Altomare, A. Leonardi, M.Tartagni, and R. Guerrieri, "A CMOS chip for individual cell manipulationand detection," *IEEE J. Solid-State Circuits*, vol. 38, no. 12, pp.2297–2305, Dec. 2003.
3. R. Yotter, L. Lee, and D. M. Wilson, "Sensor technologies for monitoringmetabolic activity in single cells—part I: optical methods," *IEEESensors J.*, vol. 4, no. 4, pp. 395–411, Dec. 2004.
4. *S.* J. Wang and J. E Chang, "Smart card basedsecure password authentication scheme,"Cumtluters *and Security,Vol. 15, No. 3,* pp. 231-237.A(1996)
5. T. Chen and A. El Gamal, "Optimal scheduling of capture times for a multiple capture imaging system," in *Proc. SPIE Electronic Imaging'2002 Conf.*, vol. 4669, Jan. 2002, pp. 288–296.
6. http://www.imoney.co.id/articles/bagaimana-cara-kerja-kartu-kredit/
7. http://www.mafiakartukredit.com/2012/03/kejahatan-kartu-kredit-re-encoded.html
8. http://mediatorinvestor.wordpress.com/artikel/kejahatan-kartu-atm-kartu-kredit/
9. (http://demo.jurnas.com/halaman/26/2013-12-03/277045), Jakarta | Selasa, 3 Dec 2013LutherKembaren
10. [;http://www.creditcard-revolution.com/bi-sebut-indonesia-masih-rawan-kejahatan-kartu-kredit/], July 11, 2012
11. (http://www.bi.go.id/id/publikasi/sistem-pembayaran/riset/Documents/4a79ad4a8dbe4ebca2c0f86a5a2f1c69KajianEMoney.pdf).
12. (http://www.bi.go.id/id/publikasi/sistem-pembayaran/riset/Documents/4a79ad4a8dbe4ebca2c0f86a5a2f1c69KajianEMoney.pdf).